

IN THE CLAIMS:

Please amend claim 1, as shown in the complete list of claims that is presented below.

1. (currently amended) A secret file access authorization system with fingerprint limitation, comprising:

an authorization server provided with an authorization module, which provides a fingerprint template and an authorization secret key, the authorization module including a password fingerprint unit, an environment fingerprint sampling unit, and a time fingerprint sampling unit, which are set in parallel, as well as an authorization unit;

an encryption server provided with an encryption module, which generates a decryption secret key by accepting the authorization secret key provided by the authorization module, and produces encrypted secret files by encrypting secret files to be encrypted;

a certification server provided with ~~the authorization~~ a certification module, which accepts the fingerprint template provided by the authorization module, accepts the decryption secret key provided by the encryption module and the authorization secret key claiming certification that is sent by a client, and judges and confirms by providing a certified decryption secret key; and

at least one client machine, each of which is provided with a user module, which embeds a kernel encryption/decryption unit into a corresponding operation system kernel of the client, accepts the authorization secret key provided by the authorization module and the decryption secret key provided by the encryption module, sends the claiming of certification respectively to ~~[[a]]~~ the certification module, opens the encryption/decryption unit with a certified authorization secret key and the certified decryption secret key which is returned after the certification module makes the certification, and reads/writes the encrypted secret files.

2. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server, the encryption server, and

the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module, and the certification module.

3. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server and the encryption server are merged to constitute an authorization-and-encryption server, which is provided with the authorization module and the encryption module.

4. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server and the certification server are merged to constitute an authorization-and-certification server, which is provided with the authorization module and the certification module.

5. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the encryption server and the certification server are merged to constitute an encryption-and-certification server, which is provided with the encryption module and the certification module.

6. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; and wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

7. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 6, wherein the authorization secret key is a binary string of a certain length.

8. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 7, wherein the authorization secret key is put into an authorized entity.

9. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 6, wherein the fingerprint template is a binary string of a certain length.

10. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

11. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 10, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

12. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 10, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

13. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the

authorization module; wherein a certification interface unit is linked with them by bidirectional programs, and also accepts the decryption secret key provided by the encryption module and a certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

14. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the user module includes an application unit, a kernel encryption/decryption unit and an input/output unit, which are linked in sequence by bidirectional programs, as well as an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for a certification module, and accepts a certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

15. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 14, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

16. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 14, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

17. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 2, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint

sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit provide the fingerprint template.

18. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 3, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

19. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 4, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit provide the fingerprint template.

20. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 5, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key,

while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

21. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 17, wherein the authorization secret key is a binary string of a certain length.

22. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 18, wherein the authorization secret key is a binary string of a certain length.

23. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 19, wherein the authorization secret key is a binary string of a certain length.

24. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 20, wherein the authorization secret key is a binary string of a certain length.

25. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 21, wherein the authorization secret key is put into an authorized entity.

26. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 22, wherein the authorization secret key is put into an authorized entity.

27. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 23, wherein the authorization secret key is put into an authorized entity.

28. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 24, wherein the authorization secret key is put into an authorized entity.

29. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 17, wherein the fingerprint template is a binary string of a certain length.

30. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 18, wherein the fingerprint template is a binary string of a certain length.

31. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 19, wherein the fingerprint template is a binary string of a certain length.

32. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 20, wherein the fingerprint template is a binary string of a certain length.

33. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 2, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

34. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 3, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

35. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 4, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

36. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 5, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

37 (previously presented) A secret file access authorization system with fingerprint limitation according to claim 33, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

38. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 34, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

39. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 35, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

40. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 36, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

41. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 33, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

42. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 34, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

43. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 35, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

44. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 36, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

45. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 2, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

46. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 3, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

47. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 4, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the

encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

48. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 5, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit linked with them by the bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

49. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 2, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein an input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

50. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 3, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification

module; and the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

51. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 4, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

52. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 5, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

53. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 49, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE

embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

54. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 50, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

55. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 51, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

56. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 52, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

57. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 49, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

58. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 50, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

59. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 51, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

60. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 52, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

61. (previously presented) A secret file access authorization system with fingerprint limitation according to claim 1, wherein the environment fingerprint sampling unit determines whether a request for decryption of one of the encrypted secret files originated from a client machine that is authorized to decrypt said one of the encrypted secret files, and wherein the time signature sampling unit determines whether said request for decryption has occurred during a limited time window set for authorized decryption.